October 17, 2008

The ABCs of Penetration Testing

Anthony Alves, Senior Systems Engineer

ABCs of Penetration Testing - Agenda

- **What is a Penetration Test?**
- **How does it relate to Vulnerability Scanning?**
- **Penetration Testing Method**
- **PT applications in the real world**
- **Final words and Q & A**

Why Penetration Testing?

- **Computer related crime is on the rise**
- **Most organizations already invest in securing their IT systems**
- **But, are they secure yet?**

Think like the enemy

- **Test your systems to see if and how they can be compromised**
- **Penetration Testing**
  - Key word is ‘systems’ not just individual machines
  - An authorized attempt to breach the security of a system by utilizing the same techniques and approaches of a real attacker
  - Ultimate check of your security utilizing the methods of a real attack
  - We are not just testing machines, but also the devices and software that should either protect your machines or warn you about the attack

A Penetration Test is not a Vulnerability Scan

- **A vulnerability scan looks for evidence of**
  - Vulnerable software/ versions
  - Presence or lack of patches
  - Common misconfigurations

- **As part of a broader vulnerability management process, scanning provides value to a maintenance function**

- **But vulnerability scanning alone is not a replacement for a test**
  - Does not tell you what an attacker can do to/on your network today
  - Does not identify dangerous trust relationships between components
  - Lots of false-positives are produced which must be manually verified
  - Only actionable items are list of missing patches

The Vulnerability Management process

Key elements of a Penetration Test

- **Answer the question ‘how secure are we?’**
- **Discover and exploit vulnerabilities throughout the network**
- **Leverage trust-relationships among components**
- **Access critical information**

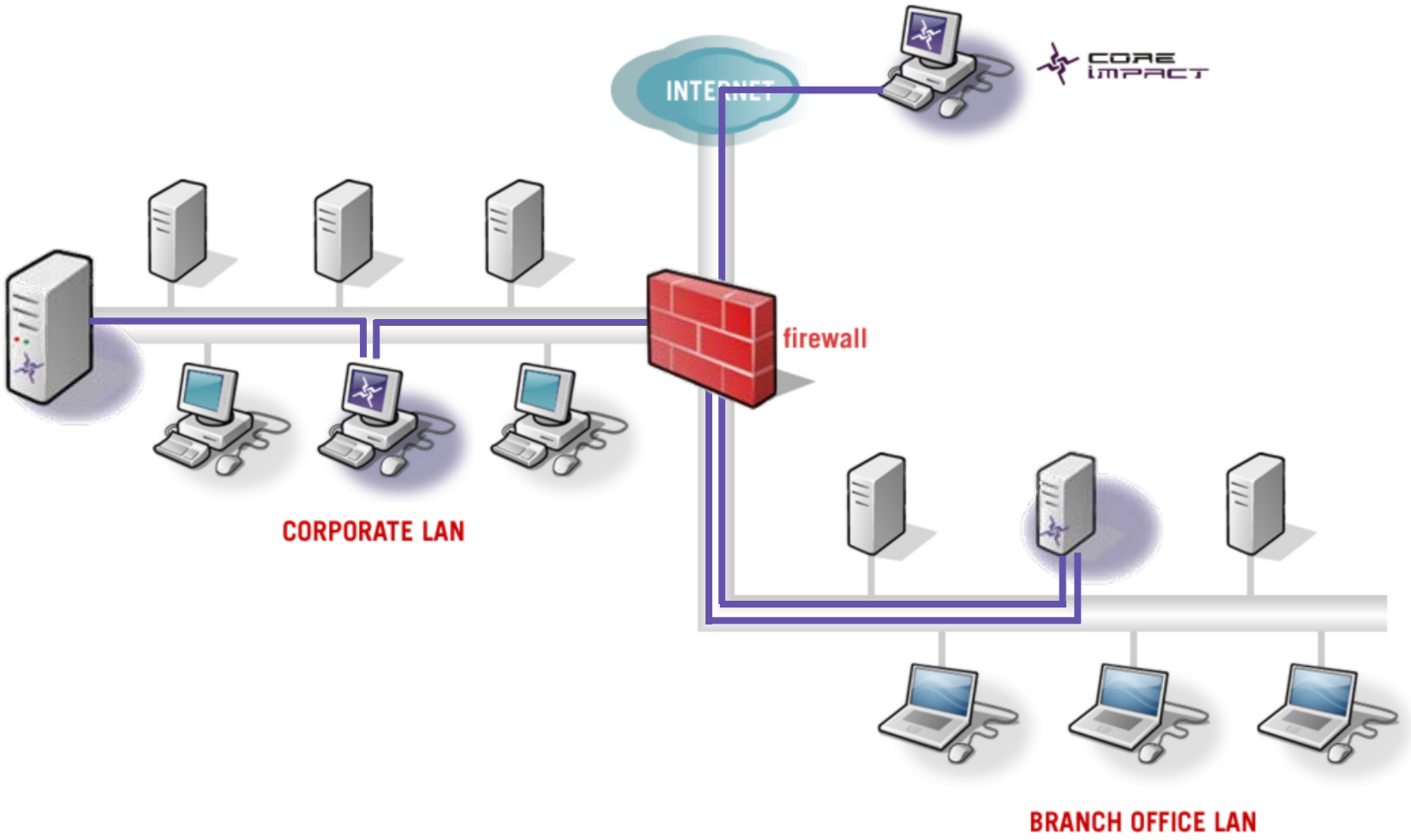
Example

"After exploiting a vulnerability in the Exchange server, we were able to collect a list of valid email user accounts and passwords. We then used this server to attack the database server in the DMZ (which wasn't visible from the outside). One of the exploits was successful and we gained administrator access to the server, including complete access to all tables in the customers database."

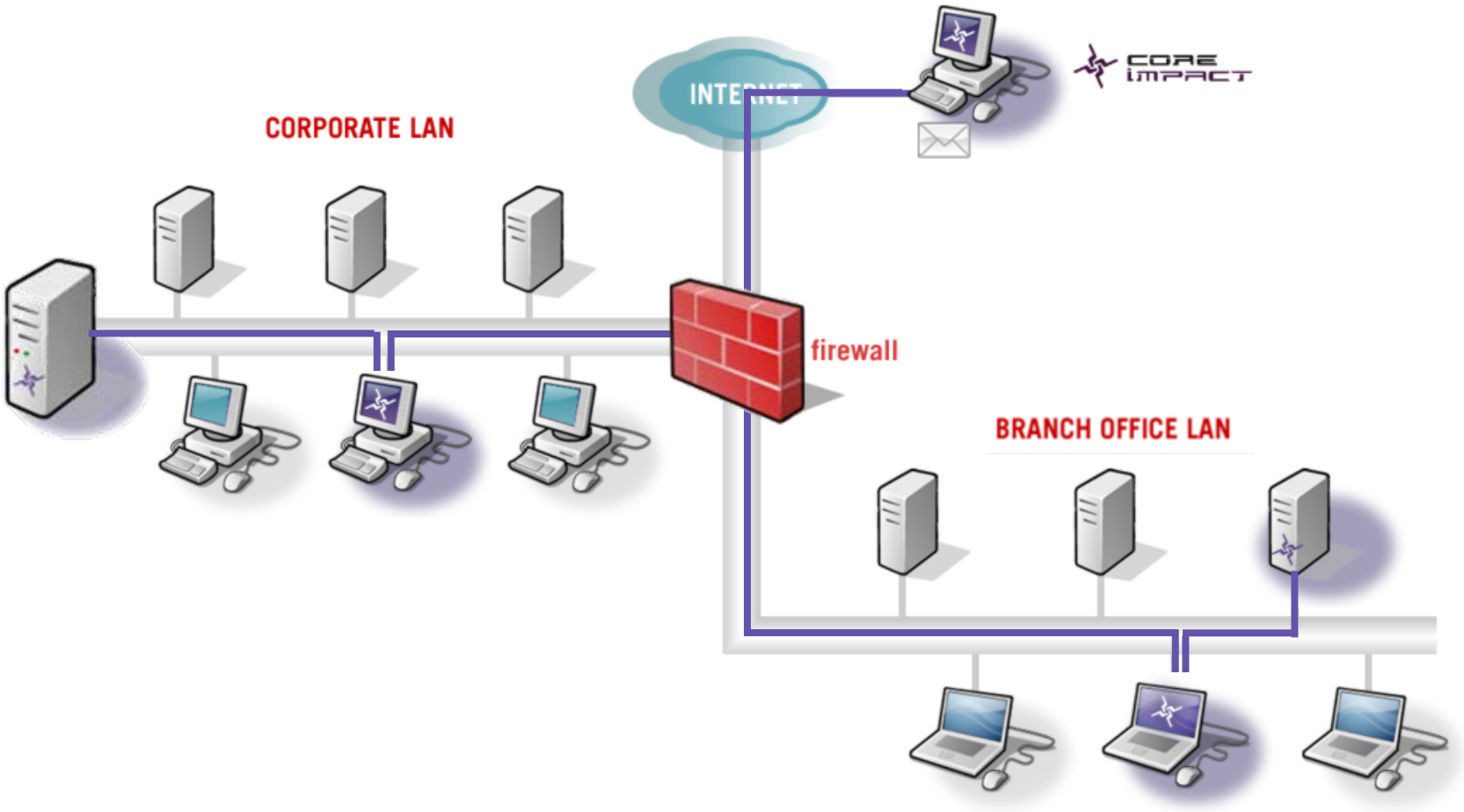
What should you test?

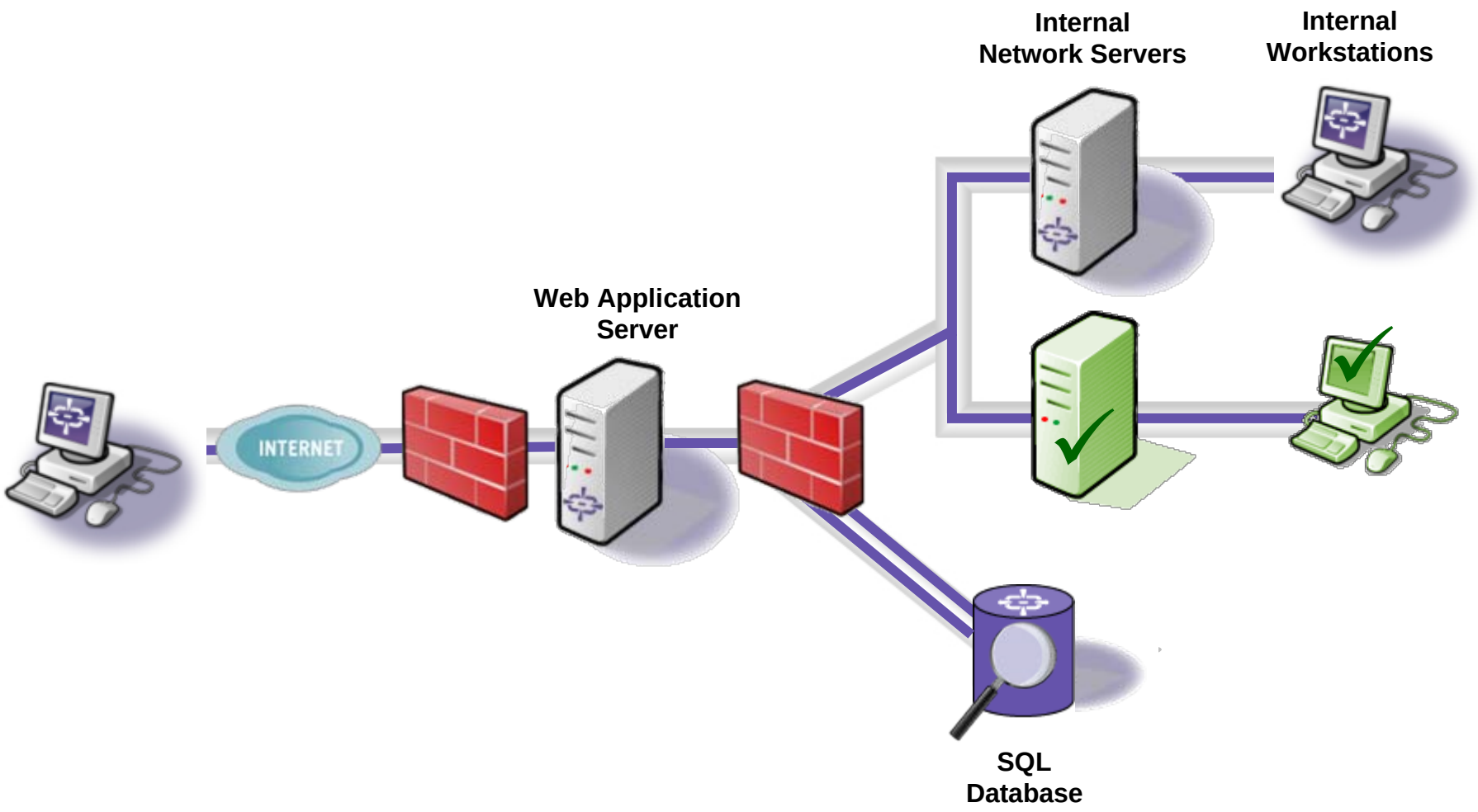
- **Test all the ways an external person can touch your network**
- **Internet facing servers (Email, DNS, Web servers etc)**
- **Users who can receive external emails**
- **Web Applications that expose data**
  - And that could expose internal systems

External Penetration Testing

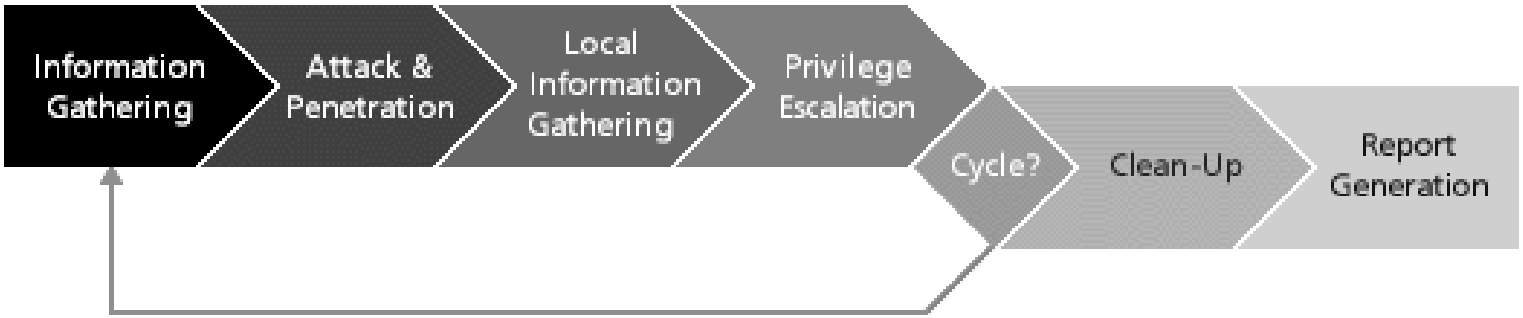


Testing via Email Attacks




Internal
Network Servers
Internal
Workstations
Web Application
Server
INTERNET
SQL
Database

The Penetration Testing process



A Good Penetration Test

- **Covers all relevant attack vectors**
- **Clearly shows how vulnerable assets can be compromised**
- **Tests the system as a whole, including existing defense mechanisms**
- **Does not disrupt business operations**
  - Unless that is part of the scope of work
- **Documents all activities performed**

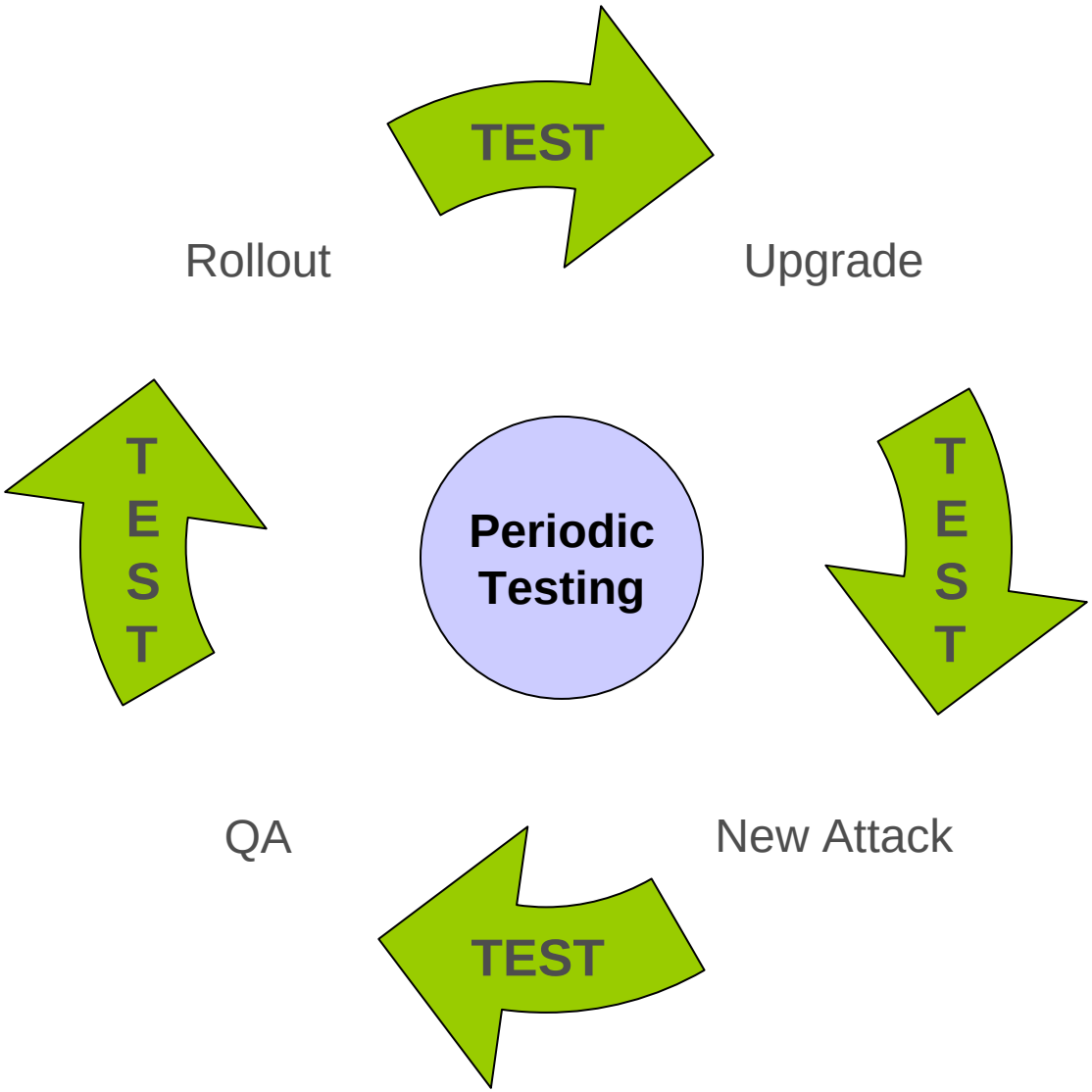
Who should do the testing

- **You could have external consultants perform the test**
  - Reliant on the skill set of the consultants
  - Cost of consultant may limit the number of times you can test

- **Have an internal team perform tests**
  - Enables more frequent testing
  - Enables better internal communication about results
  - Can also encourage people to consult with security team *before* making changes

- **What do you need**
  - Penetration Testing is now standard practice, as such commercial and free software exists
    - » www.metasploit.com free, open source Penetration Testing framework
    - » BackTrack – LiveCD with suite of tools

When is testing necessary?



How often can we test cost-effectively?

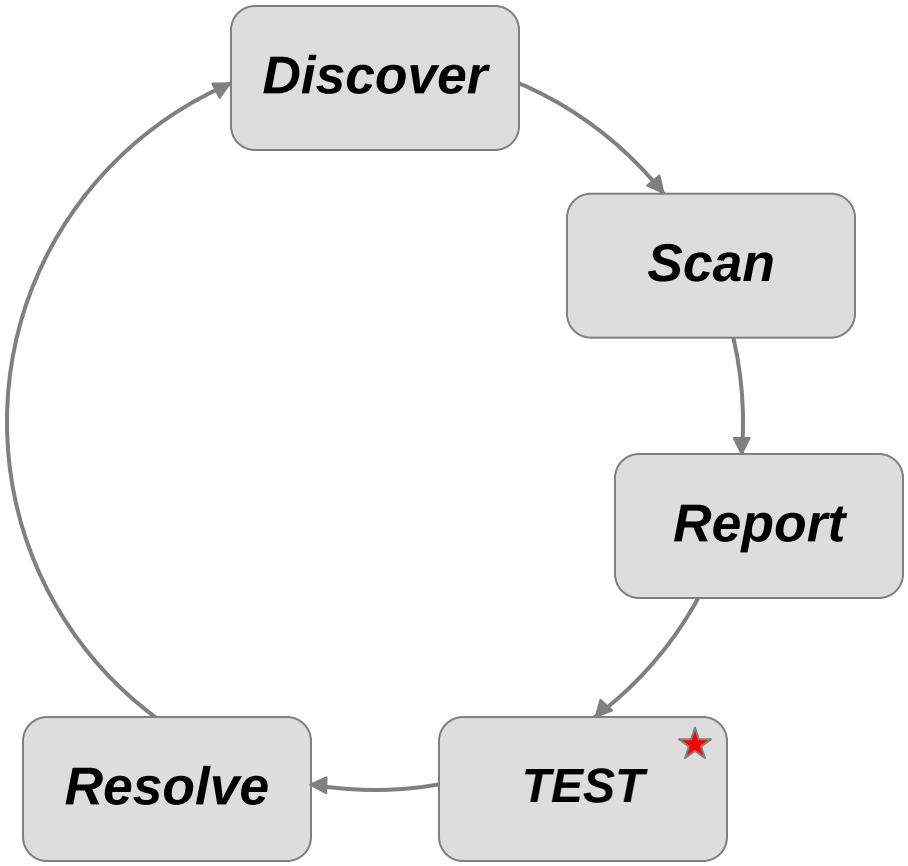
- **Penetration Testing was traditionally done once or twice a year due to high cost of service**

- **Automated Penetration Testing software is enabling organizations today to test more often**

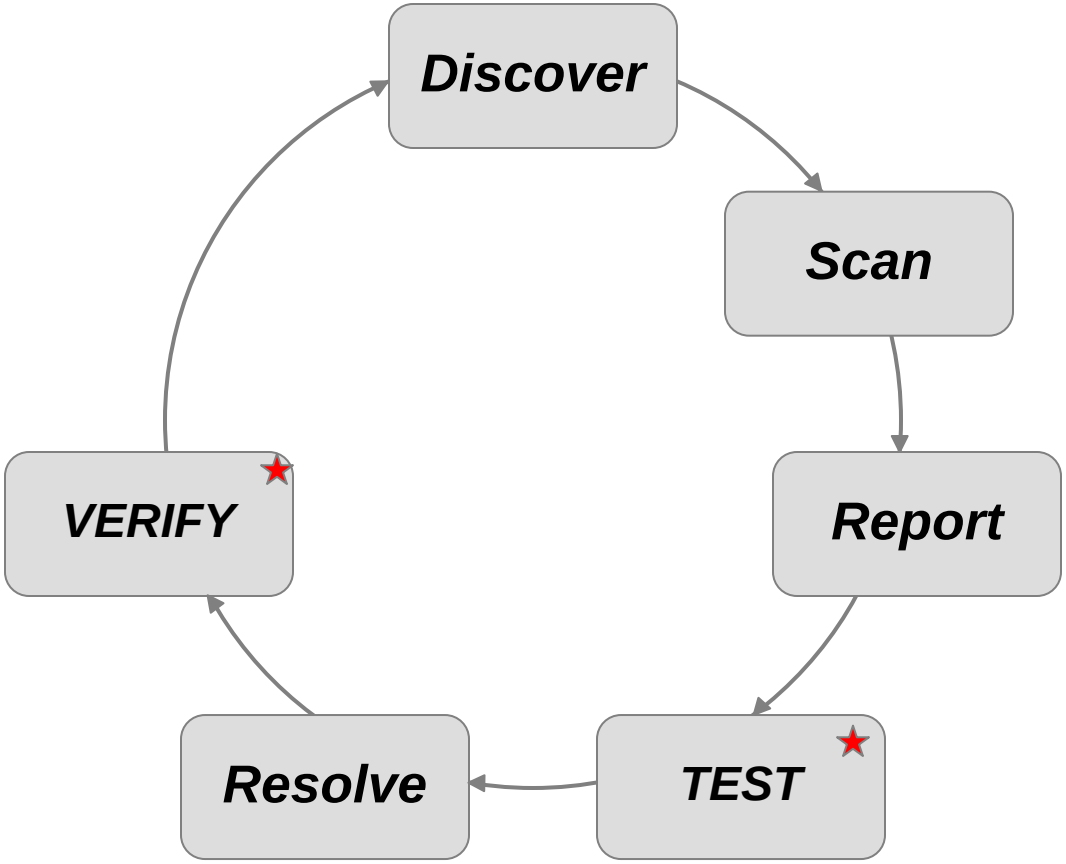
  - 75% of our customers doing testing on a monthly and weekly basis, in contrast with 50% doing it once or twice a year in late 2004

The Vulnerability Management process

Testing reduces errors and prioritizes findings



Testing verifies correct mitigation



Organizations should take advantage of both VS and PT

- **VS provides a baseline from which to start building a risk profile**
- **A Penetration Test illustrates what those vulnerabilities mean to the organization today, and can help verify remediation efforts**

Ultimately organizations just want to know what is really at risk: a Penetration Test can help answer that question

Thank You!

http://www.coresecurity.com

anthony.alves@coresecurity.com